

Standard of Decision

Article III standing is a jurisdictional requirement for a plaintiff to plead and prove. *See Steel*, 523 U.S. at 103; *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2207-08 (2021). Where, as here, standing is challenged at the pleading stage by a Rule 12(b)(1) motion, a court examines the complaint for specific facts necessary to establish standing. *Steel*, 523 U.S. at 104. “[T]he plaintiff must clearly . . . allege facts demonstrating each element” of standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)). “The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Id.*; *see TransUnion*, 141 S. Ct. at 2203. When assessing standing based only on the pleadings, a court “must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party.” *Warth*, 422 U.S. at 501.

Plaintiff’s Factual Allegations

Plaintiff is a graduate of OCU’s School of Law who now resides in Wisconsin. In July 2022 an unauthorized third party intentionally accessed OCU’s computer network and gained access to some personal information of OCU’s current and former students and employees. The exposed information potentially included Plaintiff’s name, address, social security number, driver’s license or state identification number, and passport number. In March 2023, more than eight months after the data breach, OCU sent Plaintiff a notice informing her of the cyberattack. The notice urged her to monitor credit reports for suspicious activity, contact her financial institutions, and “then take whatever steps are

recommended to protect [her] interests.” *See* Compl. ¶ 38 (quoting Ex. 1 at 2). The notice stated that OCU had no reason to believe any impacted information had been misused, but offered complimentary credit monitoring and identity protection services. *Id.* ¶ 40. Plaintiff alleges that, because of the data breach, she “now face[s], and will continue to face, a heightened risk of identity theft and fraud for the rest of [her life].” *Id.* ¶ 73.

Plaintiff brings five claims against OCU: Count I, Negligence, in failing to protect Plaintiff’s personal information and provide adequate data security; Count II, Negligence *Per Se*, in violating a provision of the Federal Trade Commission Act, 15 U.S.C. § 45; Count III, Breach of Express/Implied Contractual Duty, arising from OCU’s agreement to provide educational services or employment; Count IV, Unjust Enrichment, as an alternative to the contract claim; Count V, Invasion of Privacy, from public disclosure of private facts; and Count VI, Violation of the Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, § 751 *et seq.*, by utilizing deceptive and unfair trade practices when informing Plaintiff of the data breach. Plaintiff seeks compensatory damages and injunctive or declaratory relief for herself and a putative class of other individuals whose personal information was compromised.

Plaintiff does not allege that she or any other potential class member has been a victim of identity theft or fraud. She instead complains that her personal information “was compromised and stolen by unauthorized third parties” and consequently was “released into the public domain.” *See* Compl. ¶¶ 6, 8. As a result, she has been required to take mitigation measures “to deter and detect identity theft and fraud,” including “placing ‘freezes’ and ‘alerts’ with credit reporting agencies, contacting [her] financial institutions,

closing or modifying financial accounts, and closely reviewing [her] credit reports, financial accounts, explanations of benefits, and medical accounts for unauthorized activity.” *See* Compl. ¶ 10. Plaintiff further alleges that as a result of the data breach, she has suffered or is “at increased risk of suffering” a list of possible injuries, such as a misuse of her personal information, a loss of the opportunity to control of the use of her personal information, a diminution in the value of her personal information, an increase in spam calls and texts, and current and future costs related to the time and effort that she has expended or will expend in addressing and attempting to mitigate the data breach. *Id.* ¶ 72. Also as to damages, Plaintiff makes a conclusory allegation that, as a proximate result of OCU’s negligence, she and putative class members “have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.” *Id.* ¶ 99.

Discussion

OCU challenges Plaintiff’s Article III standing based solely on the first requirement, injury in fact. To satisfy this element, Plaintiff must show she “suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Spokeo*, 578 U.S. at 338 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).

This Court has previously considered the same question presented in this case: “Does the mere fact that a data breach occurred necessarily mean that a customer has suffered a concrete injury, or is something more required?” *See Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 989 (W.D. Okla. 2021). Lacking guidance from the Tenth

Circuit, the Court carefully considered a split of authority from the Second, Third, Fourth, Sixth, Seventh, Eighth, Ninth, Eleventh, and District of Columbia Circuits. *Id.* at 989-91. The Court also considered two Supreme Court opinions – *TransUnion* and *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013). Applying the principles distilled from these cases to the facts and claims asserted in *Legg*, this Court determined that a plaintiff suing for damages and injunctive relief from a data breach based on a risk that fraud or identity theft may occur in the future, without any facts to show a misuse of the data had occurred, failed to allege a concrete injury and lacked standing. *See Legg*, 574 F. Supp. 3d at 993-95. For the reasons explained in *Legg*, the Court found that a plaintiff who merely alleges a risk of future harm from a data breach has not shown “an actual, present injury that would support his damages claim or an imminent threat of future harm that would support his claim for injunctive relief.” *Id.* at 995.

In her brief, Plaintiff implicitly concedes that there has been no decision by the Tenth Circuit that would compel this Court to revisit its prior analysis. Plaintiff does, however, cite two intervening decisions by other federal appellate courts. After considering these developments, the Court finds them to be consistent with its prior ruling.

In *Clemens v. ExecuPharm, Inc.*, 48 F.4th 146 (3d Cir. 2022), the Third Circuit followed a prior decision (*Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011), discussed in *Legg*, 574 F. Supp. 3d at 990) but found that, unlike *Reilly*, the plaintiff’s factual allegations showed “a substantial risk that harm will occur sufficient to establish an imminent injury.” *Clemens*, 48 F.4th at 157. This finding was based on the facts that “a known hacker group named CLOP accessed [the plaintiff’s] sensitive information” – which

was “a combination of financial and personal information [that] is particularly concerning as it could be used to perpetrate both identity theft and fraud” – and affirmatively misused the information in that “CLOP had already published [the plaintiff’s] data on the Dark Web.” *Id.* at 156-57. The court concluded that “where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness [if] he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms.” *Clemens*, 48 F.4th at 155-56. The court cited as examples of such concrete additional harms, the plaintiff’s allegations that his “knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services.” *Id.* at 156. Thus, *Clemens* does not assist Plaintiff here because her Complaint does not allege facts that show a substantial risk of future harm or show that she has suffered the cited (or any other) additional concrete harms.

Similarly, in *Green-Cooper v. Brinker Int’l, Inc.*, 73 F.4th 883 (11th Cir. 2023), the Eleventh Circuit adhered to its prior rule requiring more than a data breach to confer standing on an individual whose personal information was compromised. Again, the court followed a prior decision (*Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021), discussed in *Legg*, 574 F. Supp. 3d at 991) that required the plaintiff to allege some misuse of his personal information that cybercriminals acquired from the data breach. *See Green-Cooper*, 73 F.4th at 889 (citing *Tsao*, 986 F.3d at 1343). In *Green-Cooper*, however, the court found distinguishable factual allegations. The alleged facts that “hackers took credit card data and corresponding personal information . . . and

affirmatively posted that information for sale [on the dark web] is the misuse for standing purposes that we said was missing in *Tsao*.” *Id.* at 889-90.

Like the plaintiff in *Legg*, Plaintiff here does not allege any facts that might suggest a misuse of her personal information from OCU’s data breach has occurred. As in *Legg*, Plaintiff relies primarily on a general risk of identity theft and fraudulent use of personal information due to a practice by cybercriminals of selling stolen personal information on illicit internet sites known as the “dark web.” *See* Compl. ¶¶ 45-48. Plaintiff does not allege facts from which to infer that OCU’s data breach was a targeted cyberattack to steal personal information, or that her personal information has been posted or sold on the dark web as a result of the data breach. At best, Plaintiff’s allegations permit an “inference that at some unknown time in the future, she or some of the putative class members *may* be the victim of identity theft or fraud.” *See Legg*, 574 F. Supp. 3d at 994. For the reasons fully stated in *Legg*, the Court finds that “Plaintiff only pleads facts showing that there is a non-imminent risk of possible future injury following the data breach. This is not sufficient to confer standing.” *Id.* (footnote omitted).

The Court has carefully considered the factual allegations of the Complaint and the arguments presented in Plaintiff’s brief. The Court finds no distinguishing facts or new legal arguments that would lead to a different conclusion than the one reached in *Legg*. Therefore, consistent with its prior decision in *Legg*, 574 F.3d 993-95, the Court finds that Plaintiff has failed to plausibly allege an actual, present injury that would support her claims for damages, or an imminent threat of future harm that would warrant injunctive

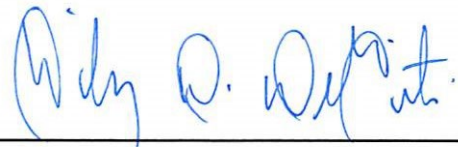
relief. Therefore, the Court finds that Plaintiff lacks standing to pursue the claims asserted in this case.

Conclusion

For these reasons, the Court finds that Plaintiff has failed to allege sufficient facts to show an actual or imminent injury that would confer standing to seek judicial relief on the claims asserted.

IT IS THEREFORE ORDERED that Defendant's Motion to Dismiss the Class Action Complaint [Doc. No. 23] is **GRANTED** as set forth herein. This action is **DISMISSED** without prejudice for lack of jurisdiction. A separate judgment of dismissal shall be entered.

IT IS SO ORDERED this 4th day of October, 2023.



TIMOTHY D. DeGIUSTI
Chief United States District Judge